Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

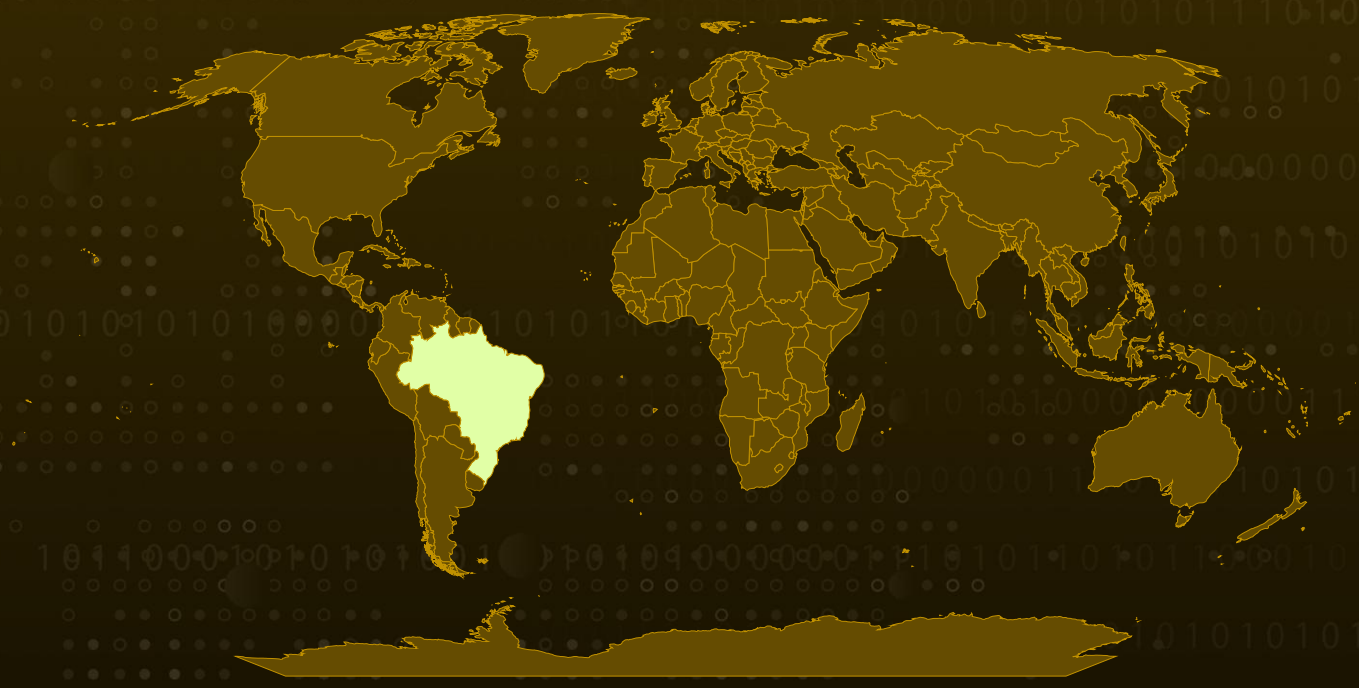
Coyote Trojan: A Digital Predator Infiltrating 70+ Financial Apps

Date of Publication	Admiralty Code	TA Number
February 4, 2025	A1	TA2025029

Summary

Attack Discovered: January 2025
Targeted Country: Brazil
Targeted Industry: Finance
Affected Platform: Windows
Malware: Coyote Banking Trojan
Attack: The Coyote Banking Trojan is a sophisticated malware strain targeting Brazilian users, engineered to steal sensitive data from over 70 financial applications and more than 1,000 websites. It operates through a stealthy multi-stage attack chain, starting with malicious LNK files embedded with PowerShell commands. These commands initiate the deployment of Coyote, which employs keylogging, screenshot capture, and phishing overlays to harvest confidential credentials and sensitive information with precision.

Attack Regions



Attack Details

#1 The **Coyote** Banking Trojan is sophisticated malware targeting Brazilian users, designed to steal sensitive data from over 70 financial apps and 1,000+ websites. Its infection chain starts with a seemingly harmless LNK file that, once clicked, silently executes PowerShell commands to connect to a remote server. This triggers the download of a malicious loader, which works with a tool called Donut to decrypt and execute the next malware stage.

#2 The decrypted payload acts as a secondary loader, running PowerShell commands to modify Windows registry keys for persistence, even after reboots. Coyote removes legitimate PowerShell entries, replacing them with disguised commands that continuously download and execute malicious code from encoded URLs.

#3 Each LNK file carries unique metadata, like a "Machine ID," helping attackers track infections. Embedded PowerShell scripts, such as "zxchzzmism," push the attack forward, while an injector DLL uses the CreateRemoteThread technique to stealthily execute additional payloads in legitimate processes.

#4 Coyote's core payload, hidden under the name "vxewhcacbfqnsw," connects to its C2 server over port 443, blending with regular encrypted traffic. It conducts system reconnaissance, monitors active windows, and targets 1,000+ websites and 73 financial institutions. When victims visit these sites, Coyote logs keystrokes, captures screenshots, and displays fake overlays to steal credentials. Stolen data is Base64-encoded and sent to the attackers.

#5 To maintain persistence, Coyote uses functions like CreateProcess to execute fresh PowerShell commands, ensuring it remains hidden and active. Its multi-stage infection chain and real-time monitoring make it a formidable threat.

Recommendations

Enhanced Email Security: Enhance email security by Implementing advanced spam filters, anti-phishing solutions, and email authentication protocols. Educate employees about identifying and reporting suspicious emails to prevent successful phishing attempts. Set up filters to catch and block suspicious LNK files and PowerShell scripts, which are common tricks cybercriminals use to kickstart an attack.

Network Segmentation and Traffic Monitoring: Continuously monitor network activity for unusual patterns, particularly connections to suspicious IP addresses, over port 443, to spot potential command-and-control (C2) communications early. which may indicate potential compromise or malicious activity.

Strengthen Financial Security: Enforce robust access controls, implement multi-factor authentication (MFA), and continuously monitor systems handling sensitive financial data to prevent unauthorized access and reduce the risk of credential theft.

Enhance Endpoint Protection: Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0009 Collection	TA0011 Command and Control
T1204 User Execution	T1204.002 Malicious File	T1059 Command and Scripting Interpreter	T1059.001 PowerShell
T1113 Screen Capture	T1056 Input Capture	T1056.001 Keylogging	T1497 Virtualization/Sandbox Evasion

T1497.001 System Checks	**T1082** System Information Discovery	**T1140** Deobfuscate/Decode Files or Information	**T1055** Process Injection
T1055.002 Portable Executable Injection	**T1112** Modify Registry	**T1547** Boot or Logon Autostart Execution	**T1547.001** Registry Run Keys / Startup Folder
T1571 Non-Standard Port	**T1027** Obfuscated Files or Information	**T1566** Phishing	**T1105** Ingress Tool Transfer
T1047 Windows Management Instrumentation			

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxps[:]//btee[.]geontrigame[.]com/mvkrouhawm, hxxps[:]//qmnw[.]daowsistem[.]com/fayikyeund, hxxps[:]//bhju[.]daowsistem[.]com/iwywybzqxk, hxxps[:]//lgfd[.]daowsistem[.]com/riqojhyvnr, hxxps[:]//leme[.]daowsistem[.]com/omzowcicwp, hxxps[:]//igow[.]scortma[.]com/fqieghffbm, hxxps[:]//quit[.]scortma[.]com/xzcpnnfhxi, hxxps[:]//llue[.]geontrigame[.]com/byyyfydxyf, hxxps[:]//cxmp[.]scortma[.]com/qfutdbtqqu, hxxps[:]//xrxw[.]scortma[.]com/gmdroacyvi, hxxps[:]//qfab[.]geontrigame[.]com/vfofnzihsm, hxxps[:]//tbet[.]geontrigame[.]com/zxchzzmism, hxxps[:]//yezh[.]geontrigame[.]com/vxewhcacbfqnsw
Domains	geraatualiza[.]com, masterdow[.]com, geraupdate[.]com
SHA256	362af8118f437f9139556c59437544ae1489376dc4118027c24c8d5ce4d84e48, 330dffe834ebbe4042747bbe00b4575629ba8f2507bccf746763cacf63d655bb, 33cba89eeeaf139a798b7fa07ff6919dd0c4c6cf4106b659e4e56f15b5809287, 552d53f473096c55a3937c8512a06863133a97c3478ad6b1535e1976d1e0d45f, 64209e2348e6d503ee518459d0487d636639fa5e5298d28093a5ad41390ef6b0,

TYPE	VALUE
SHA256	67f371a683b2be4c8002f89492cd29d96dceabdbfd36641a27be761ee64605b1, 73ad6be67691b65cee251d098f2541eef3cab2853ad509dac72d8eff5bd85bc0, 7cbfbce482071c6df823f09d83c6868d0b1208e8ceb70147b64c52bb8b48bdb8, 839de445f714a32f36670b590eba7fc68b1115b885ac8d689d7b344189521012, bea4f753707eba4088e8a51818d9de8e9ad0138495338402f05c5c7a800695a6, f3c37b1de5983b30b9ae70c525f97727a56d3874533db1a6e3dc1355bfbf37ec, Fd0ef425d34b56d0bc08bd93e6ecb11541bd834b9d4d417187373b17055c862e

References

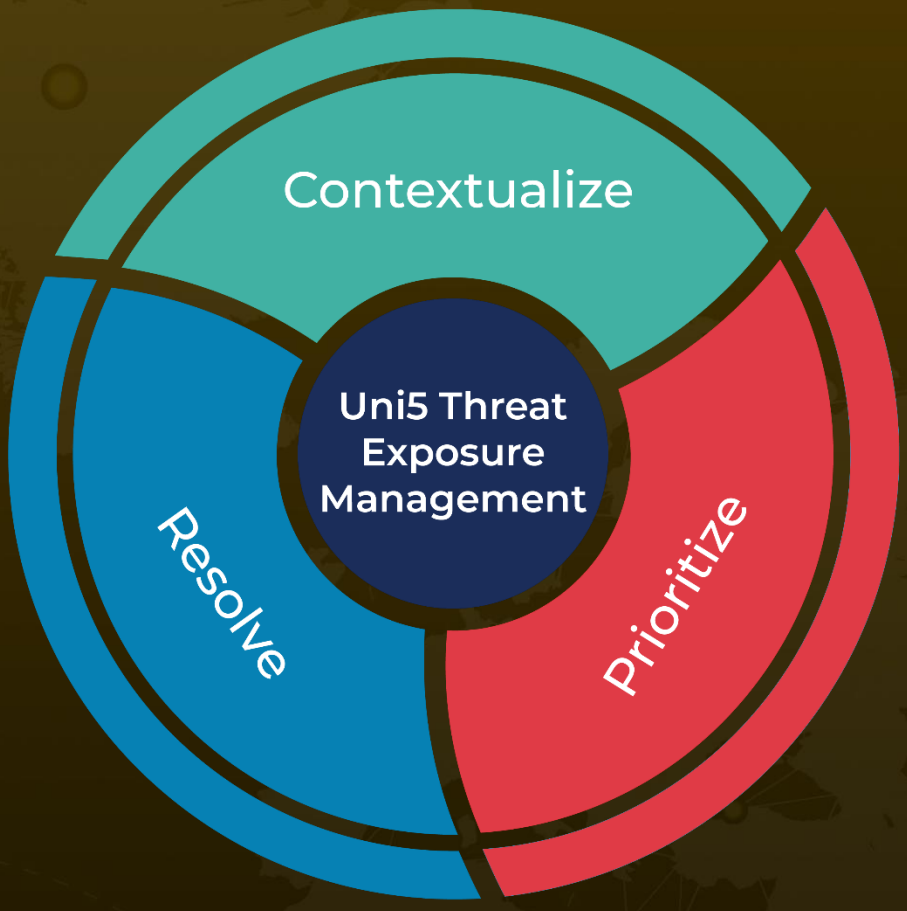
https://www.fortinet.com/blog/threat-research/coyote-banking-trojan-a-stealthy-attack-via-lnk-files

https://www.hivepro.com/threat-advisory/coyote-a-sophisticated-banking-trojan-targeting-financial-information/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

February 4, 2025 • 4:15 AM

More at www.hivepro.com